Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2017

Date filed: February 05, 2018

Name of company covered by this certification: Tri-Caps, Inc.

Form 499 Filer ID: 816370

Name of signatory: Oliver Guzman

Title of signatory: President

I, Oliver Guzman, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the Company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 CFR §64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, record keeping, and supervisory review) set forth in section 64.2001 et seq. of the Commission rules.

The Company **has not** taken any actions (i.e., proceedings instituting or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

The Company **has not** received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47.C.F.R. § 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may be subject it to enforcement action.

Signed: 

/s/ Oliver Guzman
Oliver Guzman
President
Tri-Caps, Inc.

TRI-CAPS, Inc.

Accompanying Statement to Annual 47 C.F.R. § 64.2009(e) CPNI Certification
EB Docket No. 0636

Tri-Caps, Inc. ("the Company") takes the protection of Customer Proprietary Network Information ("CPNI") seriously. The Company has retained legal counsel to advise it in this area and has taken the following steps to protect the confidentiality of its customers' information and to ensure compliance with the Commission's CPNI rules.

1. It is the Company's policy not to use, disclose, or permit access to CPNI, as defined in the FCC's rules, for any purposes except the following, all of which are permitted without customer approval by the FCC's rules:
    a. To initiate, render, bill, and collect for services; and
    b. To protect the rights or property of the Company, or to protect users of its services from fraudulent, abusive, or unlawful use of, or subscription to, such services.
2. As a condition to their employment, employees must agree, in writing, that they will not, directly or indirectly, disclose confidential information to any third person, firm or company during or after their employment with the Company. Such confidential information includes CPNI. If an employee fails to comply with this requirement, he or she will be subject to disciplinary action, which may include dismissal from the Company.
3. During calendar year 2017, the Company did not engage in any outbound marketing using CPNI. No future outbound marketing campaign is currently planned nor can it be conducted without management approval and any such campaign would require supervisory review to assure compliance with the CPNI rules.
4. Because the Company does not use, disclose or permit access to CPNI (except as described above) it does not maintain a record of sales and marketing campaigns that use customers' CPNI, or of instances where CPNI is disclosed to third parties, or where third parties were allowed access to CPNI.

5. Because the Company does not use CPNI (except as described above), the Company does not utilize a notification and customer approval process (*i.e.*, Opt-Out or Opt-In process). If the Company changes its marketing procedures and begins to use CPNI in ways other than specified in paragraph 1 above, an appropriate customer notification process will be instituted.

6. The Company provides no online customer access for CPNI of any kind.

7. The Company does not release customers' CPNI (either in-person or over the phone) without first establishing that the person requesting the information is either the customer whose CPNI is being requested or an authorized user.

8. The Company protects CPNI databases from unauthorized access by implementing two separate sets of passwords, firewalls, and encrypted billing files. Furthermore, only the Company's President and General Manager are provided with access to CPNI databases.

9. The Company has not detected any unauthorized access to CPNI, either by employees, pretexters or other third parties. The Company did not receive any customer complaints regarding CPNI in 2017.

10. Had there been a breach of a customer's CPNI as described in section 64.2011 of the FCC's rules, the Company would have, as soon as practicable and in all events within seven (7) days of the determination of the breach, notified law enforcement through http://www.fcc.gov/eb/cpni, and subsequently notified the customer(s), in accordance with the procedures and in the sequence prescribed by that rule section. The Company would have maintained a record of any such breaches and notifications for at least two (2) years.